DEC 2016

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the December 2016 edition of In the Boxing Ring

This month, we discuss the **Changing Landscape of Cyber Security**. Over the last twelve months, one thing that has been abundantly clear is that the front lines of security are becoming more complex. Cyber attacks are also growing in numbers and above all else, the attacks are growing in terms of speed and volume. On pages 2-3 we discuss these issues in greater detail, and try to anticipate what to expect in 2017 and beyond.

On page 4, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, Network Box is proud to announce that the M-Series won a **SMBWorld 2016 Award** for *Best Security Solution (Hardware)*. Network Box Hong Kong also welcomed some members of the **Network Box Germany** team for an update on the latest Network Box 5.3 features, and the **HKTDC** was at Network Box HQ to film a series of videos featuring Network Box.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
December 2016

You can contact us here at HQ by email (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

The Changing Landscape of CYBER SECURITY

As 2016 closes, it seems a good time to look back and see what has changed in the security landscape, as well as try to anticipate what we have to look forward to in 2017 and beyond.

One thing that has become abundantly clear is that the front lines of Internet Security are becoming more complex. Up until recently, we put our servers in a DMZ, workstations in a LAN, and did all that we could to defend them on a single front of perimeter security – with attacks primarily coming from the Internet. Nowadays, however, all that is changing; servers are in the cloud and our users are on mobile devices out on the streets. Now we're fighting the battle on at least three fronts. Ask anyone with military experience and they will tell you that is not a good position to be in; you have to defend all those places, while the attackers have to just find one area of weakness.

The old days of brute force attacks and network vulnerabilities are thankfully mostly behind us. We've learned to patch regularly, and the Internet has helped us easily obtain and install those patches (often in an automated manner). But we now have a huge number of Internet Connected Devices – from light bulbs to door locks – and those devices are often riddled with vulnerabilities, have back doors, and are not so easy to apply security patches to.

The attacks are also growing in sophistication. The old days of blatantly obvious phishing emails have gone, and we are now faced with perfectly phrased persuasive messages that confuse even experts as to their authenticity. One click, and a stream of exploits are downloaded to install ransomware that can then spread over the local network behind firewall protection. If an expert cannot easily tell whether these are fake or real, how can a junior office staff be expected to know?

And above all else, the attacks are growing in speed. I am reminded of that line in Top Gun when Commander Stinger is told the aircraft launch catapults are broken and will take 10 minutes to fix; his reply of 'Bullshit ten minutes! This thing will be over in two!' reflects the problem facing the network security industry nowadays. We're used to and comfortable with the technology of signature protection – but even drastically reducing the time to producing and releasing those signatures from hours to minutes will make little difference to an attack that runs to completion in two minutes. Take any zero-day malware and upload to virustotal.com; it is common that none of the 50+ mass-market anti-malware engines have protection for at least the first hour of the attack. The malware writers simply test their creations are undetected, prior to release to millions of targets within seconds, via huge botnets of compromised hosts.

As for 2017 and beyond?

...more of the same.

Sure, we can increase the speed of our signature release (Network Box pioneered the move from pull to push signatures – decreasing release times from days/hours to 45 seconds or less). We can remove the need for signature release entirely by leaving the signatures in the cloud and doing real-time lookups (Network Box addresses this with our Z-Scan engines) and that brings the protection deployment time from first sample down to 2 or 3 seconds. We can even remove the need for signatures altogether by heuristic / emulation technology (Network Box has several heuristic engines in our Network Box 5 product today). But, even with all that, we are not addressing the core fundamental problem that to succeed, we need to defend against 100% of attacks successfully, while to fail the attacker only needs to get through ONCE.

Network Box has been preaching for years now that the solution to these new threats to the security landscape is a change from signature based to policy based protection. The Network Box 5 system is at its heart, a classification and policy engine. We look at streams of network data (email messages, web downloads, etc) and classify them (spam, ham, malware, executable, dlp, etc). Policy is then applied to permit/deny the transfer, and it is the effectiveness of that policy that is the key to the security of the assets it is protecting.

The Network Box anti-spam and anti-malware engines do an incredible job at detecting such malicious data streams, and use dozens of protection technologies including heuristics, emulation, zero-day cloud based signatures, reputation lookup, as well as signature protection delivered by push updates. We even offer SSL interception and decryption options to be able to do this within encrypted streams.

Despite the changing security landscape, our recommendation today remains the same as it was ten years ago:

- Customers should move from relying solely on blacklist based policies (where everything is allowed through except for that scanned to be malware / undesirable), to a whitelist based policy (where executable and otherwise suspicious content is denied, except from those specifically whitelisted senders).
- At the firewall level, we've moved from 'allow all, but block tcp/22' to 'deny all, but allow tcp/80'. Most have now also moved to similar whitelisted based policies outbound.
- But, at the stream level, we are still allowing executable content into our network. We need to move to a policy where executable content is blocked (blacklisted), except from specific trusted senders (whitelisted).

It is the role of Network Box Security Operation Centers to help you enforce that policy.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th December 2016, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
December 2016

This month, for Network Box 5, these include:

- Introduction of a command line console level 1 cache, for startup performance improvement
- Support for query source IP address in DNS server
- Support for numbered (with IP address) IPv4 GRE tunnels
- OpenSSL security updates
- Comments now permitted in rule style configurations
- Provide an option to bypass frontline protection for incoming IPSEC connections
- Performance improvements for VPN logging and reporting queries
- Add multi-home support for SSL VPN servers
- Add support to add routes via ACL for SSL VPNs
- Performance and reliability improvements for NOC servers, when contacting boxes over unreliable links
- Support redirection of ports 4242,4243,4244, and 4245 for admin.network-box.com and user.network-box.com
- Improve statistics calculation methodology for mail summary when a particular email has multiple classifications
- Improved support for Anti-DDoS collections in generic, IMAP, POP3, and SMTP protocols
- Support good/bad transaction count factors in Anti-DDoS collections
- Improved process monitoring for authentication scanning engine
- Improved process monitoring for file scanning engine
- Improved support for scanning large email attachments and mime sections, in particular for DLP and SPAM classifications
- Improved support for ACE archive format
- Provide an option to temporarily blacklist sender, if a mail is caught in a spam trap
- Provide an policy option to enforce envelope and 'from' header senders match

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

SMBWorld Awards 2016

Network Box won an SMBWorld Award 2016, for Best Security Solution (Hardware), for the Network Box M-Series cyber-security platform. Network Box Managing Director, Michael Gazeley collected the award on behalf of the company at the awards ceremony that took place at The Cordis, Hong Kong.

Network Box Hong Kong HKTDC Video Interview

The HKTDC (Hong Kong Trade Development Council) was at Network Box HQ to film a six episode series, featuring Network Box, and the IT and Security Landscape.

Network Box Germany HQ Visit

Network Box HQ welcomed some of our team from Network Box Germany, to be updated on the latest features and functionalities, included with Network Box 5.3.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com